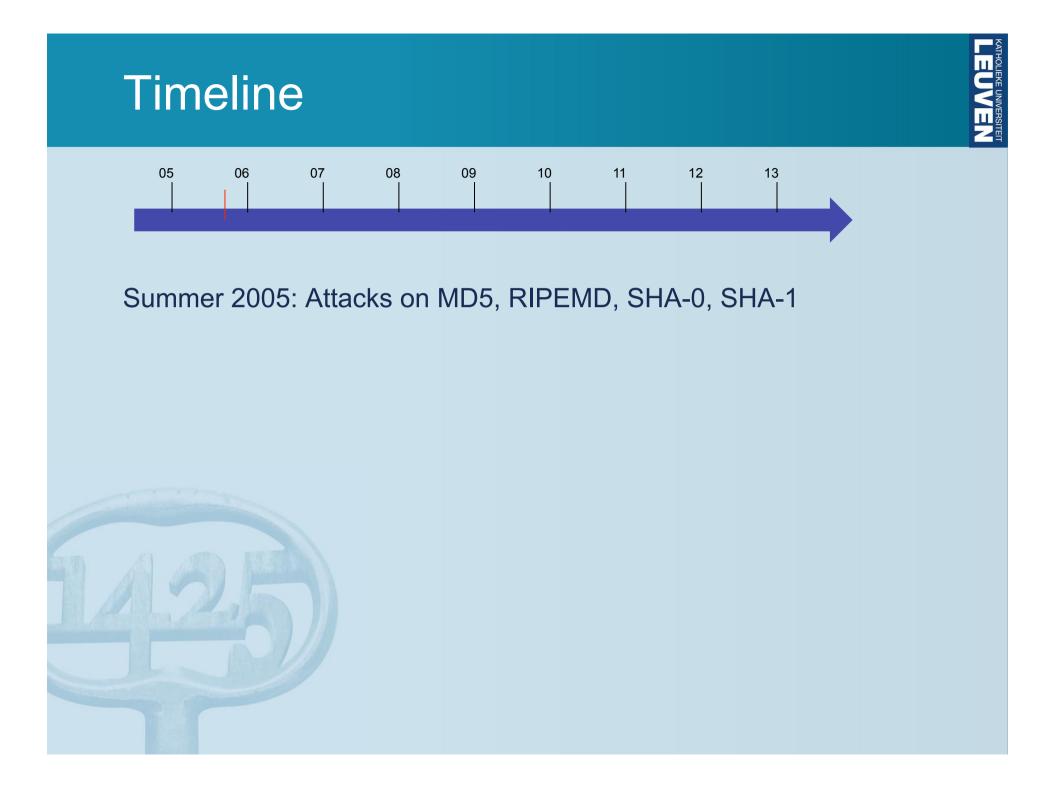






The SHA-3 Process

Keccak & SHA-3 day Brussels, 27 March 2013



The Wang effect

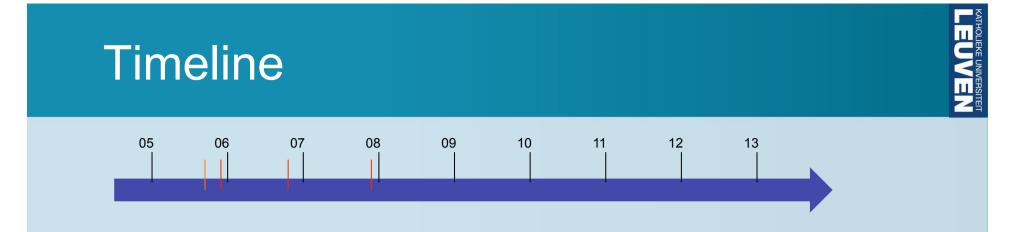
Before 2005

- MD4 (Dobbertin)
- MD5 (Boss., Den Boer)
- SHA (Chabaud-Joux)
 SHA (days)
- SHA-1
- SHA-2

After Wang

- MD4 (seconds)
- MD5 (hours)
- SHA-1 (months (?))
- SHA-2 (?)

We need a competition like for the AES!



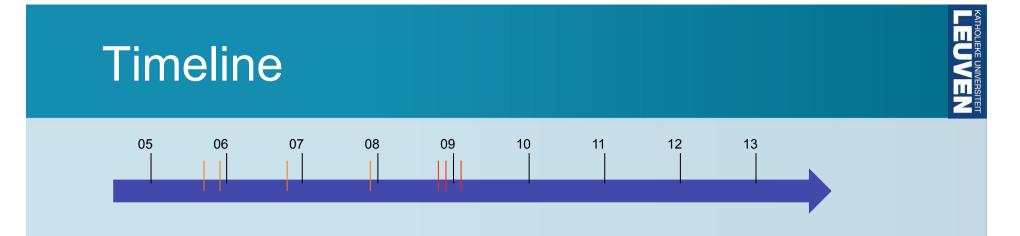
Nov 2005: 1st NIST workshop Aug 2006: 2nd NIST workshop Nov 2007: Start of the competition



NIST call: requirements

- To support 3 digest lengths: 256, 384, 512
- Should work with HMAC
- Resistance against collision, preimage attacks, ...
 - Length extension attacks, ...

- "Look" random
- Sufficiently different from SHA-2
- Let the games begin ...

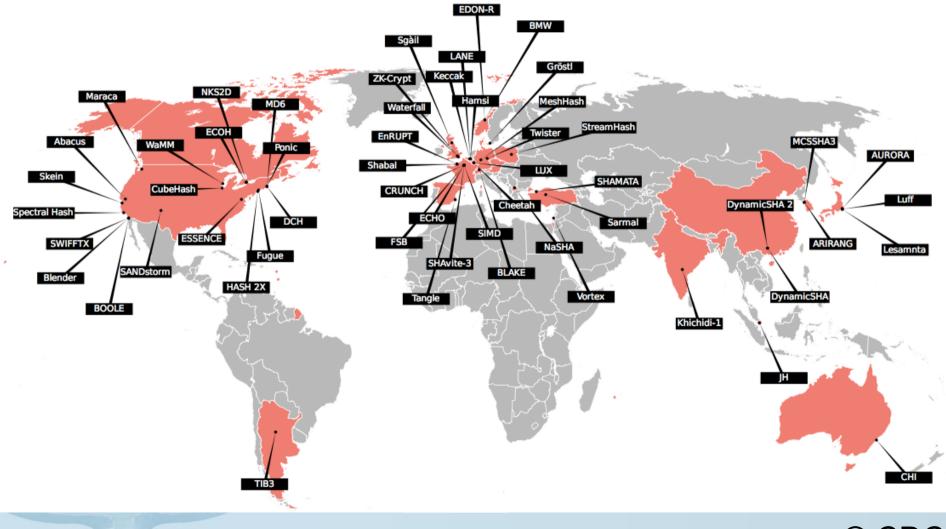


Oct 2008: End of submission (64) Dec 2008: Start of round 1 (51) Feb 2009: 1st SHA-3 candidate conference



Submissions

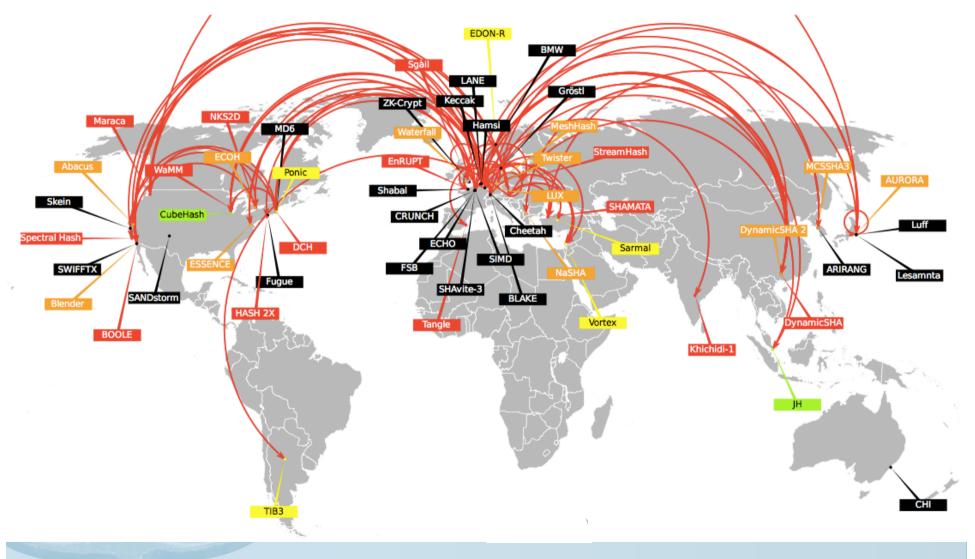




© CDC

The battlefield





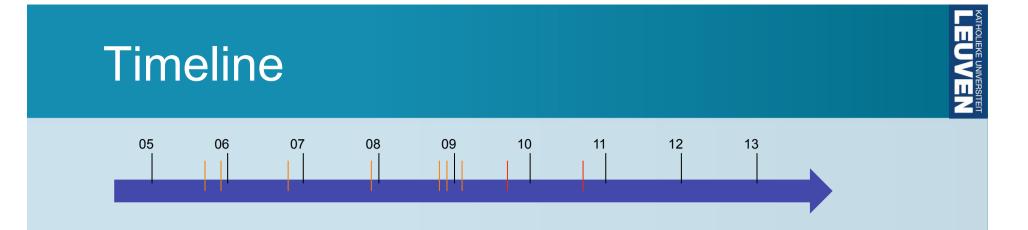
© CDC

Round 1 victims (+ Round 0)



	Abacus	Neil Sholer	2nd-preimage			
	ARIRANG	Jongin Lim				
	AURORA	Masahiro Fujita	2nd preimage			
	Blender	Colin Bradbury	collision, preimage			
	Boole	Greg Rose	collision			
	Cheetah	Dmitry Khovratovich				
	CHI	Phillip Hawkes				
	CRUNCH	Jacques Patarin				
	DCH	David A. Wilson	collision			
	Dynamic SHA	Xu Zijie	collision			
	Dynamic SHA2	Xu Zijie	collision			
	ECOH	Daniel R. L. Brown	2nd preimage			
	Edon-R	Danilo Gligoroski	preimage			
	EnRUPT	Sean O'Neil	collision			
	ESSENCE	Jason Worth Martin	collision			
	FSB	Matthieu Finiasz				
	HASH 2X	Jason Lee	2nd-preimage			
	Khichidi-1	M. Vidyasagar	collision			
	LANE	Sebastiaan Indesteege				
	Lesamnta	Hirotaka Yoshida				
	LUX	lvica Nikolić	collision, 2nd preimage			

Maraca	Robert J. Jenkins	preimage					
MCSSHA-3	Mikhail Maslennikov	2nd preimage					
MD6	Ronald L. Rivest						
MeshHash	Björn Fay	2nd preimage					
NaSHA	Smile Markovski	collision					
NKS2D	Geoffrey Park	collision					
Ponic	Peter Schmidt-Nielsen	2nd-preimage					
SANDstorm	Rich Schroeppel						
Sarmal	Kerem Varıcı	preimage					
Sgàil	Peter Maxwell	collision					
SHAMATA	Orhun Kara	collision					
Spectral Hash	Çetin Kaya Koç	collision					
StreamHash	Michal Trojnara	collision					
SWIFFTX	Daniele Micciancio						
Tangle	Rafael Alvarez	collision					
TIB3	Daniel Penazzi	collision					
Twister	Michael Gorski	preimage					
Vortex	Michael Kounavis	preimage					
WaMM	John Washburn	collision					
Waterfall	Bob Hattersley	collision					
ZK-Crypt	Carmi Gressel						
ehash.iaik.tugraz.at/wiki/The SHA-3 Zoo							



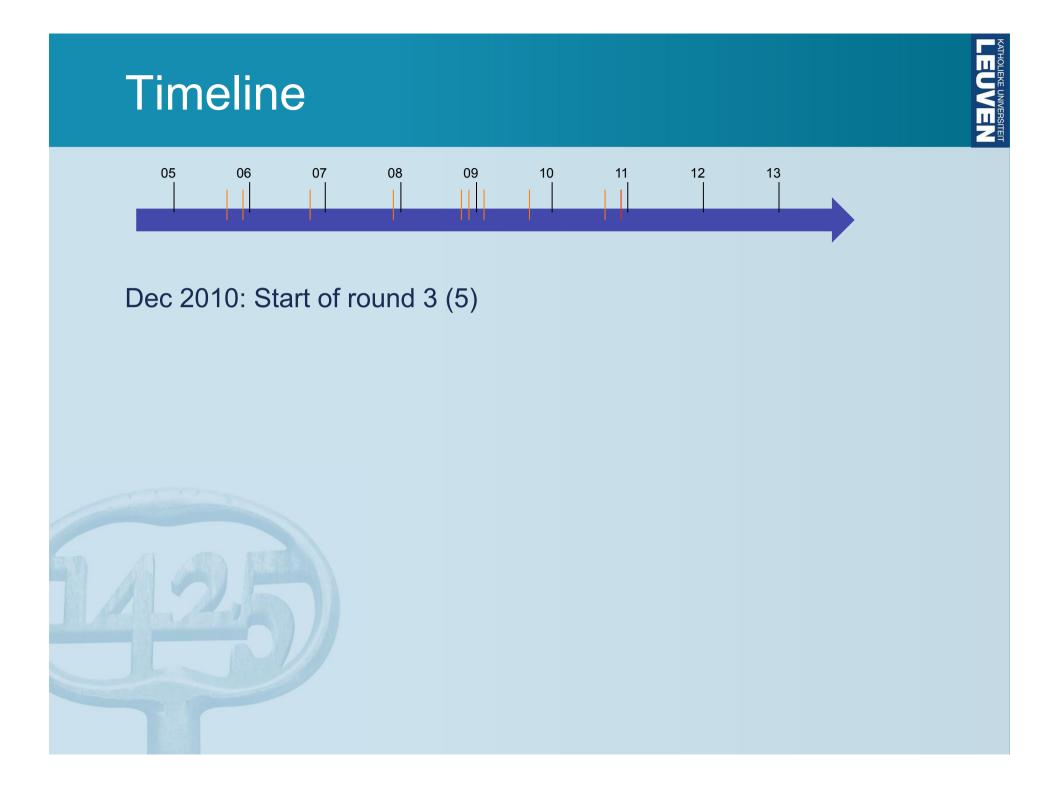
July 2009: Start of round 2 (14) Aug 2010: 2nd SHA-3 candidate conference



Round 2 victims



Blue Midnight Wish	Svein Johan Knapskog	
CubeHash	Daniel J. Bernstein	preimage
ECHO	Henri Gilbert	
Fugue	Charanjit S. Jutla	
Hamsi	Özgül Küçük	
Luffa	Dai Watanabe	
Shabal	Jean-François Misarsky	
SHAvite-3	Orr Dunkelman	
SIMD	Gaëtan Leurent	



The 5 finalists

- Blake
 - JP Aumasson, L Henzen, W Meier, RCW Phan
- Grøstl
 - P Gauravaram, LR Knudsen, K Matusiewicz, F Mendel, C Rechberger, M Schläffer, SS Thomsen
- JH
 - H Wu
- Keccak
 - G Bertoni, J Daemen, M Peeters, G Van Assche
- Skein
 - N Ferguson, S Lucks, B Schneier, D Whiting, M Bellare, T Kohno, J Callas, J Walker

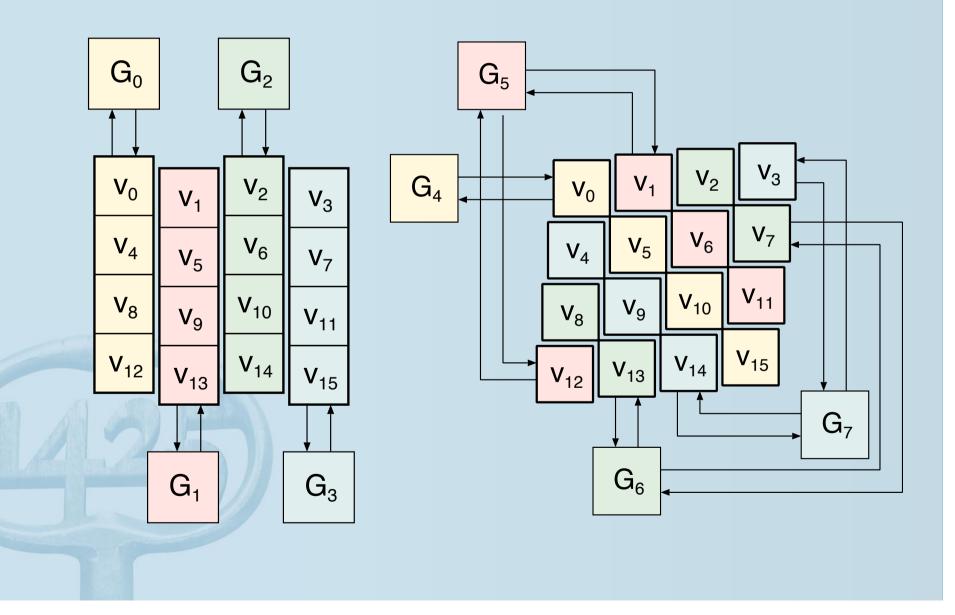


Blake Local wide-pipe • finalization next initialization rounds chain value chain value salt salt counter message

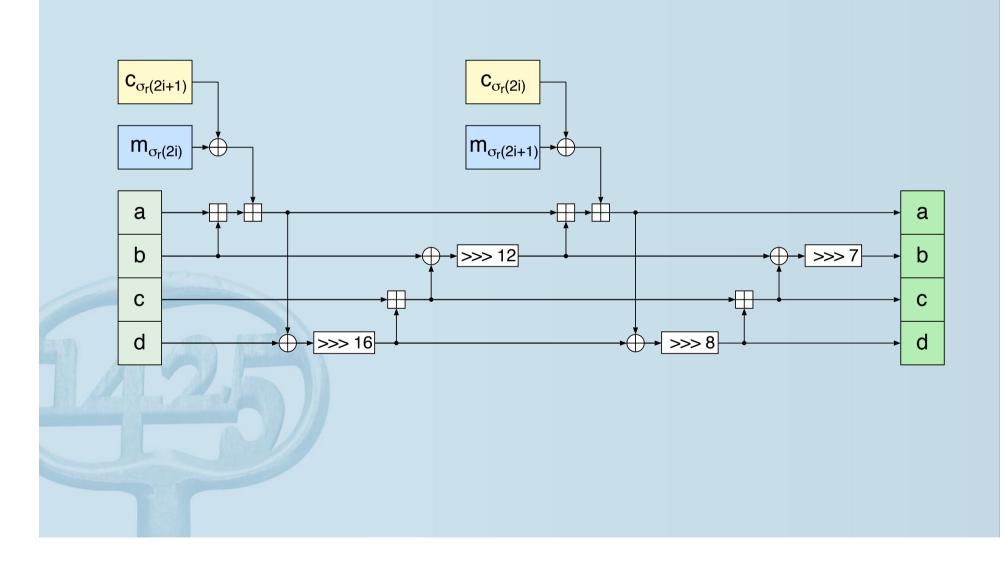
- Round function inspired by Salsa, Chacha
- 14/16 rounds







Blake G-function (1/8-round)



Blake features

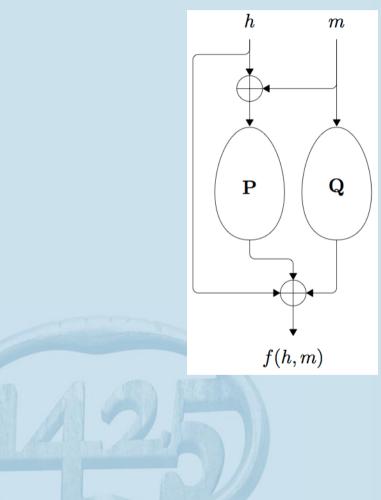
- ARX
- Many rounds and fast
- Learned from mistakes in Lake









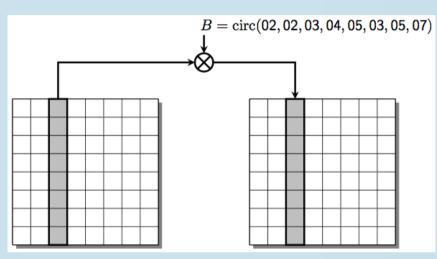


AddRoundConstant SubBytes ShiftBytes MixBytes							
IVIIXDytes							
		+	+	-			
				-			
			1				
		+		-			

• 10/14 rounds

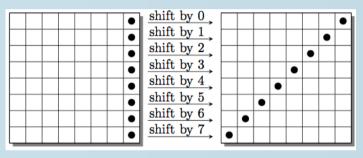
"AESsy" operations

MixBytes



SubBytes

ShiftBytes



• •	
---	--



Grøstl features

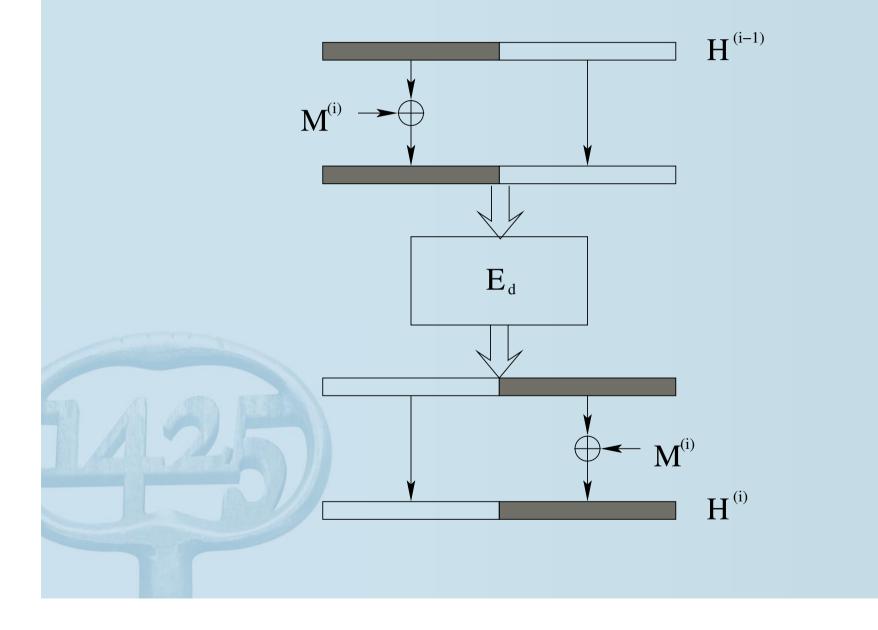
- Substitution-Permutation Network
- Fast when AES instructions available
- Permutation-based design

- Problem with "internal differential" attack
 - Solved by tweak



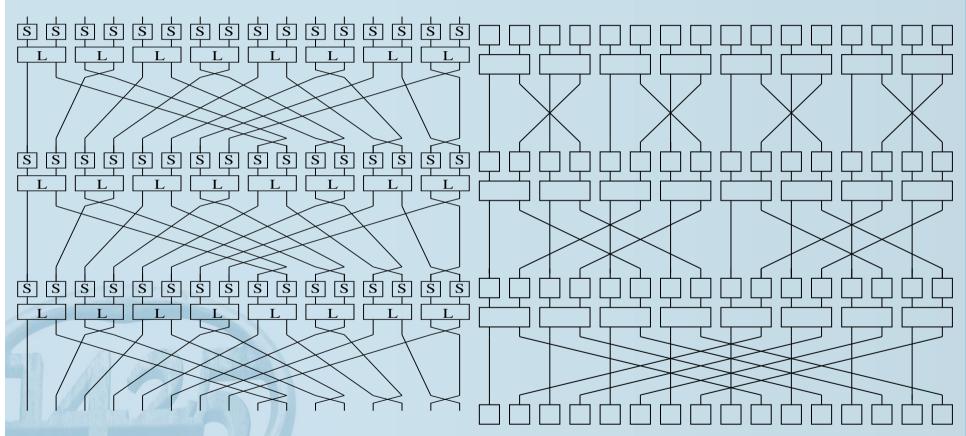








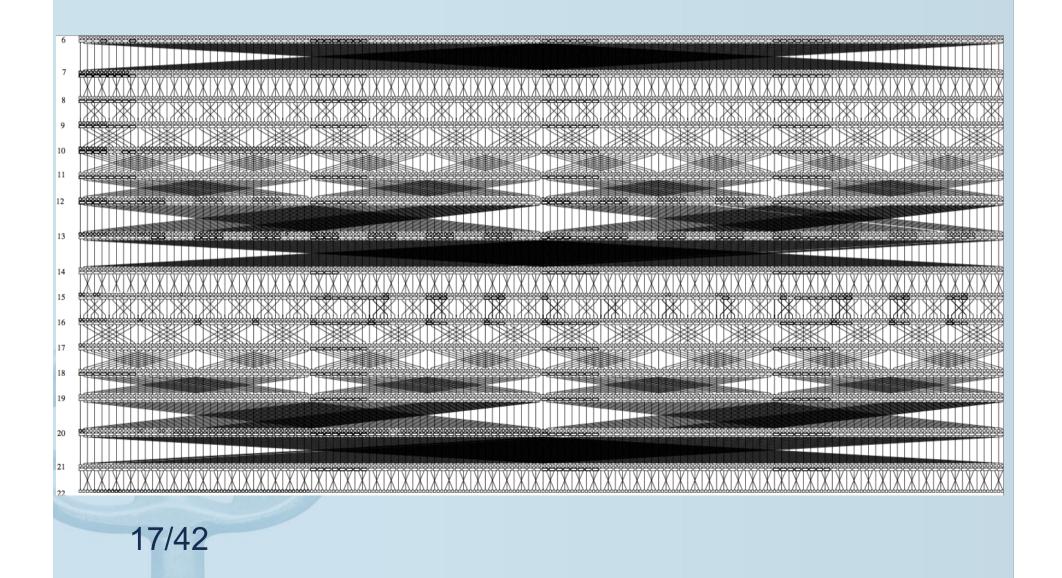




- 4-bit S-boxes (2)
- 2-input MDS layer

JH more rounds





JH features

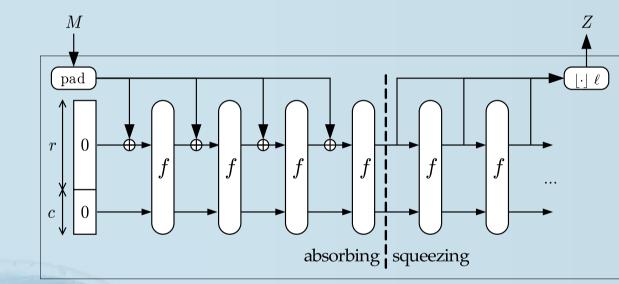
- "ShiftRows" different from AES
 - Bounds on characteristics
- Comparatively low speed
- Rebound attack on full function (42 rounds)
 - Distinguisher









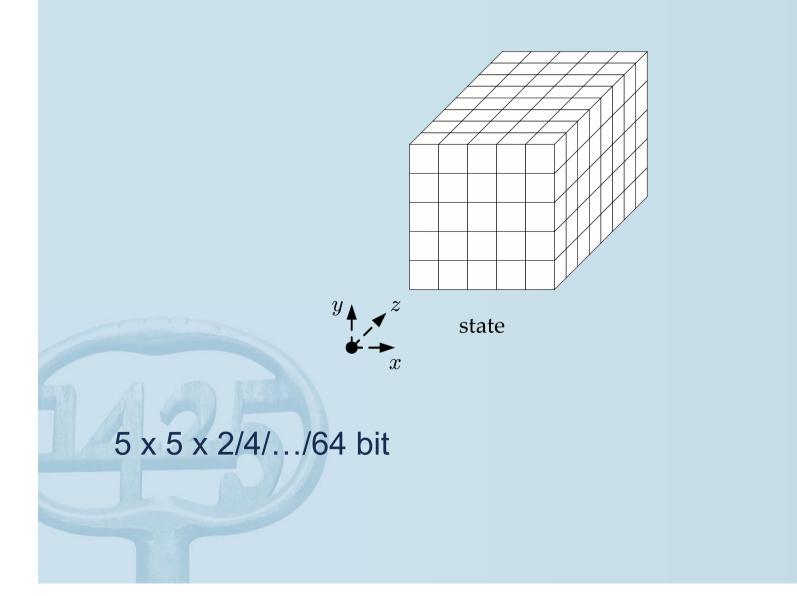


sponge

Sponge24 rounds

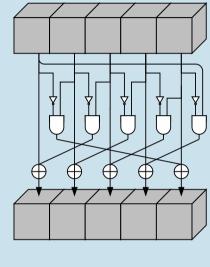


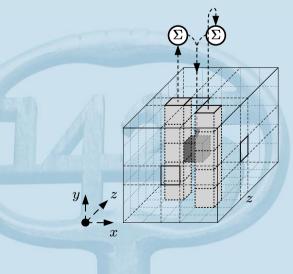


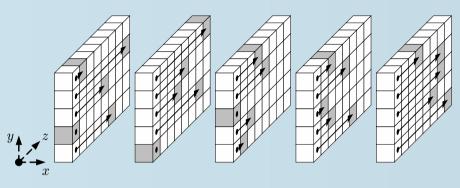


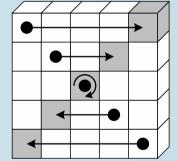
Keccak round steps

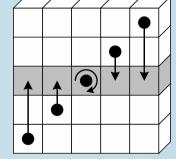


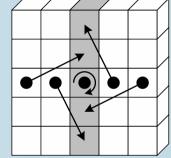


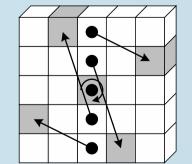


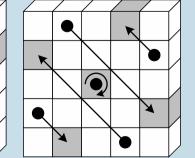


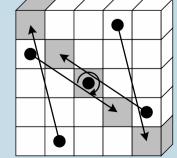












Keccak features

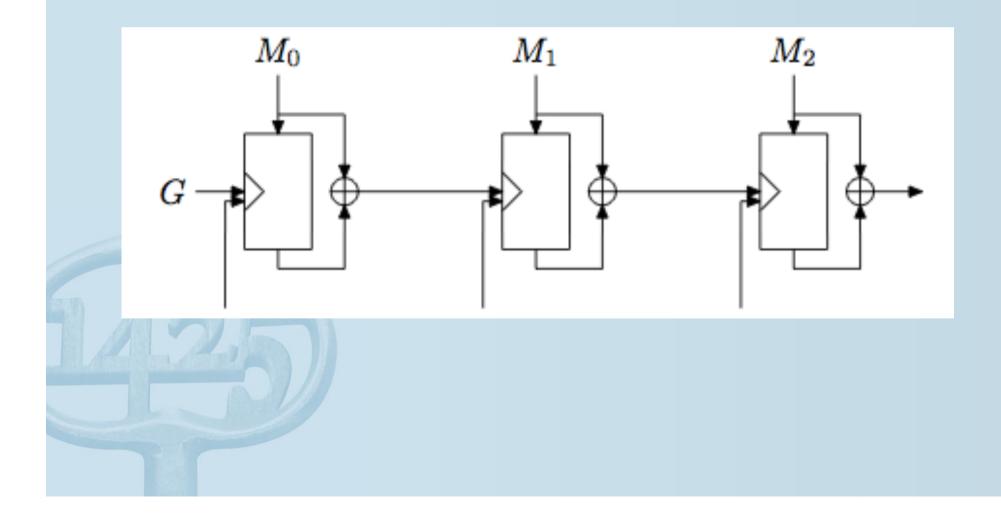
- Sponge: permutation-based
- Resembles 3D Cellular Automata
- Speed: in the middle





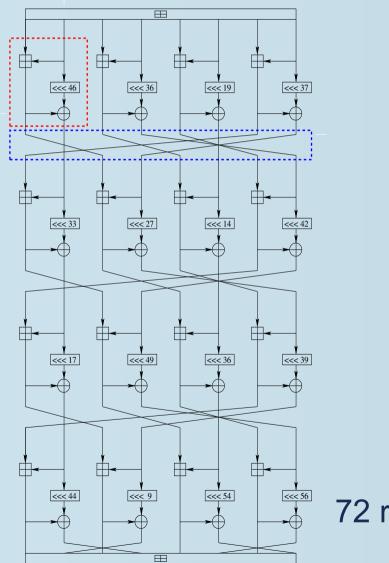
Skein: Unique Block Iteration (UBI)

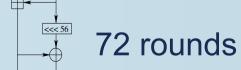
Mode of operation for a tweakable block cipher



Skein: Threefish









Skein features

KATHOLIEKE UNIVERSITEIT

- ARX
- Very many rounds and fast
- Threefish is very different from Blowfish, Twofish





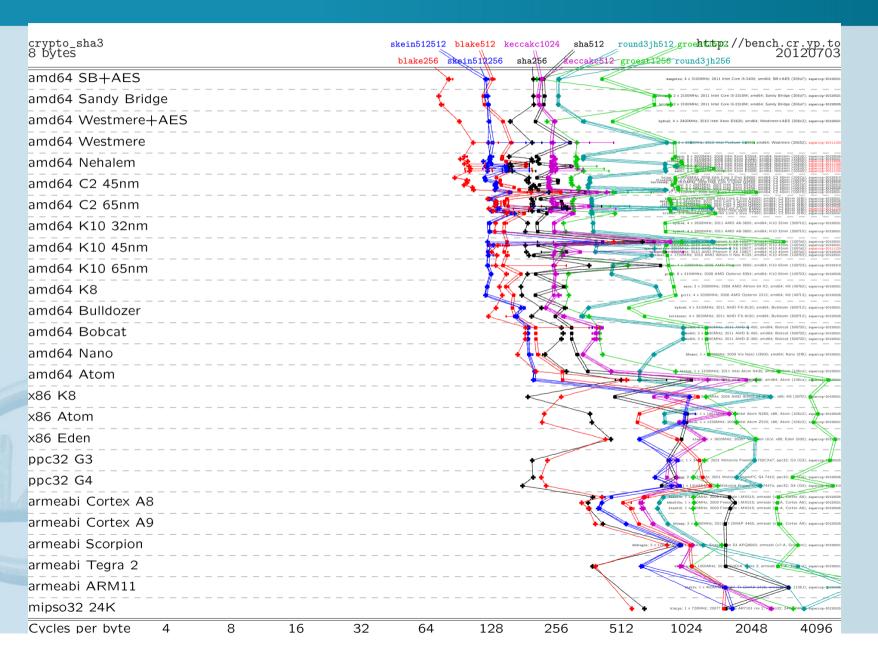






crypto_sha3 Long messages _{skein}	skein512512 512256 plake2			24round3jh512 g				http	o://bench. 2	cr.yp.to 0120703
amd64 SB+AES	+	+						mangetsu; 4 × 3100MHz; 2011	Intel Core i5-2400; amd64; SB+A	ES (206a7); supercop-20120521
amd64 Sandy Bridge	e							h6sandy; 2 x 2100MHz; 2011 Intel bridge; 2 x 2100MHz; 2011 Intel		
amd64 Westmere+A	ES	+ + +						hydra2; 4 x 2400MHz; 2010 Intel :	Keon E5620; amd64; Westmere+A	ES (206c2); supercop-20120521
amd64 Westmere								bazinga; 2 × 2800MHz; 2010 Int	el Pentium G6950; amd64; Westm	ere (20652); supercop-20111120
amd64 Nehalem								dragogicki drve v svo ogo	9 Intel Xeon E5504, amd64, Neha 9 Intel Xeon E5504, amd64, Neha 9 Intel Xeon E5504, amd64, Neha 9 Intel Xeon E5504, amd64, Neha	em (19645); supercor-20120525 Em (19655); supercor-20120525 Em (19655); supercor-30140545 Em (18645); supercor-3014118
amd64 C2 45nm				.				uess?; 4 × 2128MH2; 200 being; 2 × 3000MH2; 2008 Intel being; 2 × 3000MH2; 2008 Intel being; 3 × 3000MH2; 2008 Intel being; 4 × 248MH2; 2008	9 Intel Xeon E5506; amd64; Neha Core 2 Duo E8400; amd64; C2 45 Ste 2 Dua E8400; amd64; C2 45 Ste 2 Dua E8420; amd64; C2 45	mm (19635); sapercop-20120310 nm (19672); sapercop-20120310 nm (19672); sapercop-20120312 sapercop-20120312 sapercop-20120312
amd64 C2 65nm								Action 2 2 2 2100MHz 2005 Intel katana 2 2 2100MHz 2005 Intel katana 2 2 2107MHz 2005 Intel 12002 1 2 2004 Inte 12002 1 2 2004 Inte 12002 1 2 2004 Intel 12002 1 2 2004 Intel 12005 1 2 2005 Intel 12005 1 2 2 2005 Intel 12005 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	eL Core 2 Duo 168230; 3m362; 22 38 re Core 2 Duo 16600; am64; 22 45 Core 2 Duo 66600; am64; 22 Core 2 Buad Beses am64; 22	nm (10876); supercol-20120521 supercol-20120521 65nm (610); supercol-20120521 supercol-20120521 88nm (810); supercol-20120521 supercol-20120521
amd64 K10 32nm	/>		2->					trident; 2 x 2000MHz; 2007 Int	1 AMD A6-3650; amd64; K10 32r	85nm (866); supercop-20120521 m (300/10); supercop-20120521
	· – – <u>– – –</u> –	· - <u> - \ + +</u> - +	M					hydra5; 4 × 2900MHz; 201 henon; 6 × 2800MHz; 2010 AMD Pher dyna3; 6 × 3800MHz; 2010 AMD Pher	1 AMD A8-3850; amd64; K10 32r tom II X6 1055T; amd64; K10 45r tom II X6 1100T; amd64; K10 45r	m (300f10); supercop-20120521
amd64 K10 45nm	🐴 🐔						agan 2	emon; 6 × 3200MHz; 2010 AMD Pher ydra1; 6 × 3200MHz; 2010 AMD Pher h3mec; 1 × 1700MHz; 2010 AMD At ranger; 4 × 2200MHz; 2008 AN		Im (100fa0); supercop-20111120 Im (100fa0); supercop-20120525 Im (100f63); supercop-20120521
amd64 K10 65nm		<u>>_}_+ - </u>						goc16; 8 × 2194MHz; 2008 AM	D Opteron 8354; amd64; K10 65r	m (100f23); supercop-20120525
amd64 K8				1					2006 AMD Athlon 64 X2; amd64; 2006 AMD Opteron 2212; amd64;	
amd64 Bulldozer			24						11 AMD FX-8120; amd64; Bulldos 11 AMD FX-8150; amd64; Bulldos	
amd64 Bobcat								b4e450; 2 × 1650MH	2; 2011 AMD E-450; amd64; Bobo 2; 2011 AMD E-450; amd64; Bobo 2; 2011 AMD E-450; amd64; Bobo	at (500f20); supercop-20120521
amd64 Nano									2: 2011 AMD E-350; amd64; Bobc 	Nano (6f8); supercop-20120521
amd64 Atom			- <u>-</u> - /	+	<u> </u>			h4atom; 1 x 1330MHz;	2011 Intel Atom N435; amd64; At	om (106ca); supercop-20120521
x86 K8								h2atos; 1 × 1000MHz;	2010 Intel Atom N455; amd64; At	om (106ca); supercop-20120521
		·			<u> </u>				2004 AMD Athlon 64 3800+; x86	: K8 (20ff2); supercop-20120521
x86 Atom		L							Iz; 2009 Intel Atom N280; x86; At Iz; 2008 Intel Atom Z520; x86; At	
x86 Eden						7		hleden; 1 × 160	DMHz; 2006? Via Eden ULV; x86;	Eden (6d0); supercop-20120521
ppc32 G3		• •				•		biomol; 1 × 349MHz; 2001	Motorola PowerPC 750CXe?; ppc	32; G3 (G3); supercop-20120525
ppc32 G4			¥					gggg: 2 × 533MHz; 2001	Motorola PowerPC G4 7410; ppc	32; G4 (G4); supercop-20120525
armeabi Cortex A8									Motorola PowerPC G4 7447a; ppc: Freescale i.MX515; armeabi (v7-A, Freescale i.MX515; armeabi (v7-A,	
armeabi Cortex A9				·				h1mx515; 1 × 800MHz; 2009	Freescale i.MX515; armeabi (v7-A,	Cortex A8); supercop-20120525
			<u> </u>		#					
armeabi Scorpion							hidragen;	2 x 1782MHz; 2011 Qualcomm Snapd	ragon S3 APQ8060; armeabi (v7- <i>i</i>	A, Scorpion); supercop-20120521
armeabi Tegra 2								h6tegra; 2 × 1000MHz; 2	010 NVIDIA Tegra 2; armeabi (v7-	A, Tegra 2); supercop-20120521
armeabi ARM11								diablo; 1 × 400MHz	; 2006? TI OMAP 2420; armeabi	(v6, 1136J); supercop-20120225
mipso32 24K				+ + 4				himips; 1 x 720MHz; 2007?	Atheros AR7161 rev 2; mipso32;	24K (24Kc); supercop-20120525
Cycles per byte	4 8	16	32	64	128	256	512	1024	2048	4096

eBASH figures (short messages)



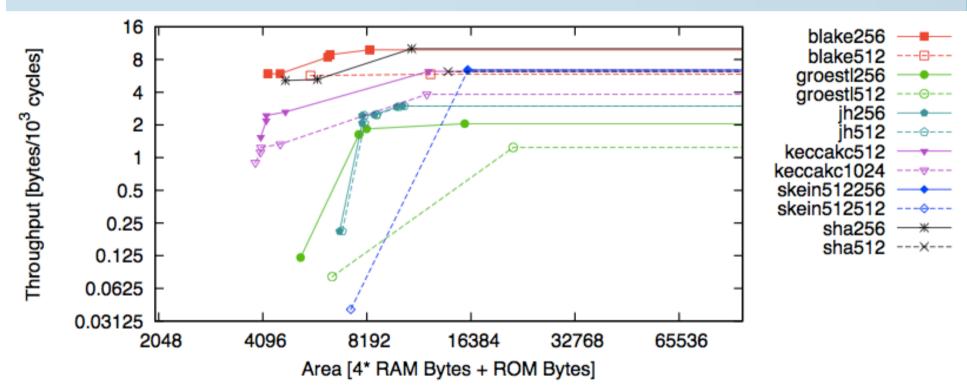
eBASH speed conclusions

- Skein and BLAKE are the fastest
- Grøstl and JH are the slowest
- Keccak and SHA-256 in the middle

- ARX trumps S-boxes
 - Even with AES instruction extensions



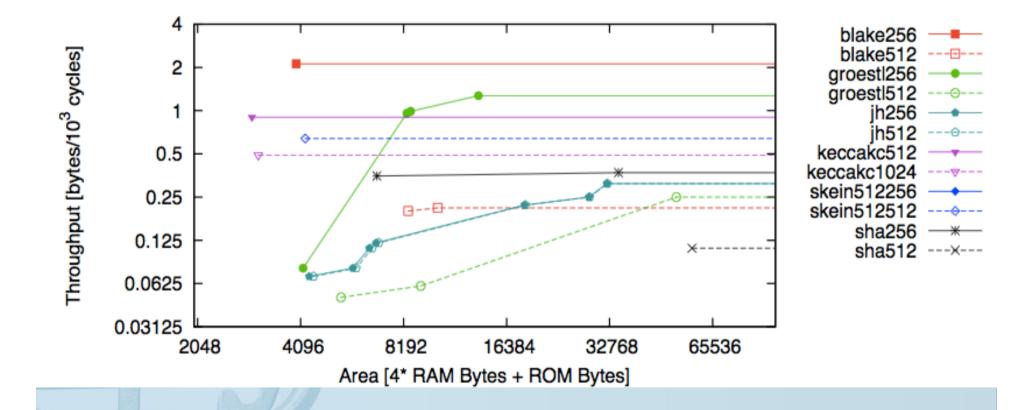
XBX figures: AR7 (32-bit)

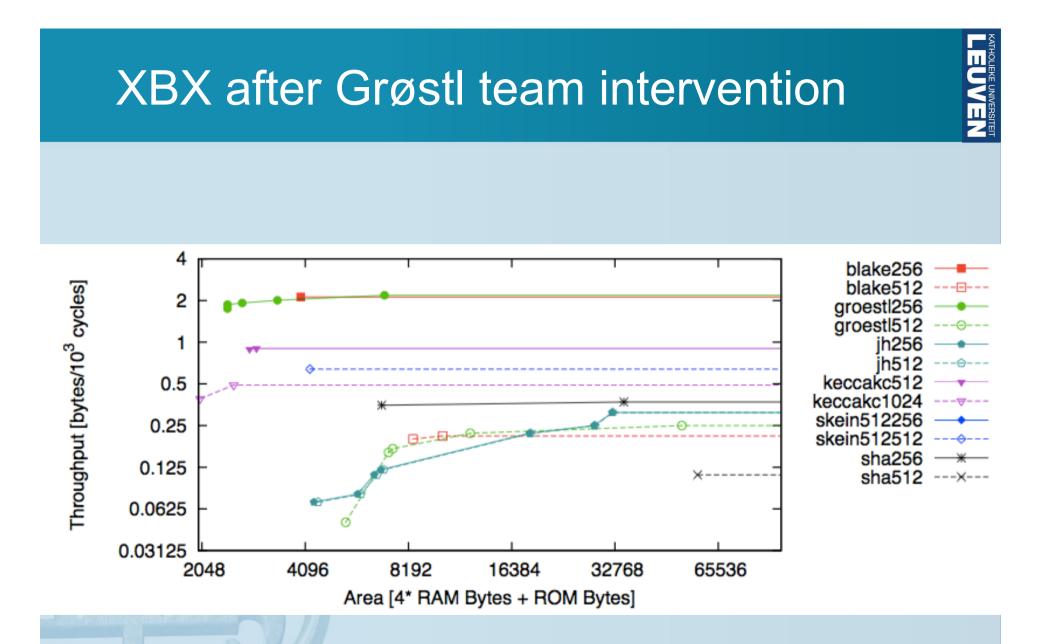






XBX figures: ATmega1284P (8-bit)





XBX figures conclusions

- Minimum required area can be more important than speed
- BLAKE always among the best
 - Skein is the best on high-end platforms
- Keccak and Grøstl repeatedly among the best
- Figures depend greatly on effort spent

Minimal Sizes



256-bit	State size (+FF)	Message block	Rounds
BLAKE	512 (+ 1024)	512	14 (x2)
Grøstl	1024 (+512)	512	10
Keccak	1600	1088	24

	512-bit	State size (+FF)	Message block	Rounds
	BLAKE	1024 (+ 1024)	1024	16 (x2)
	Grøstl	2048 (+1024)	1024	14
	JH	1024 (+512)	512	42
6	Keccak	1600	576	24
	Skein	512 (+1024)	512	72

SHA-3 key words

- Rebound
- Attack complexity/practicality
- Distinguisher nonrandom property
- Provable security indifferentiability





Remember the AES Key words?

- Security-margin weighted performance
- Side-channel attack resistance
- Algebra
- Pronunciation of Dutch vowels



Rebound attack

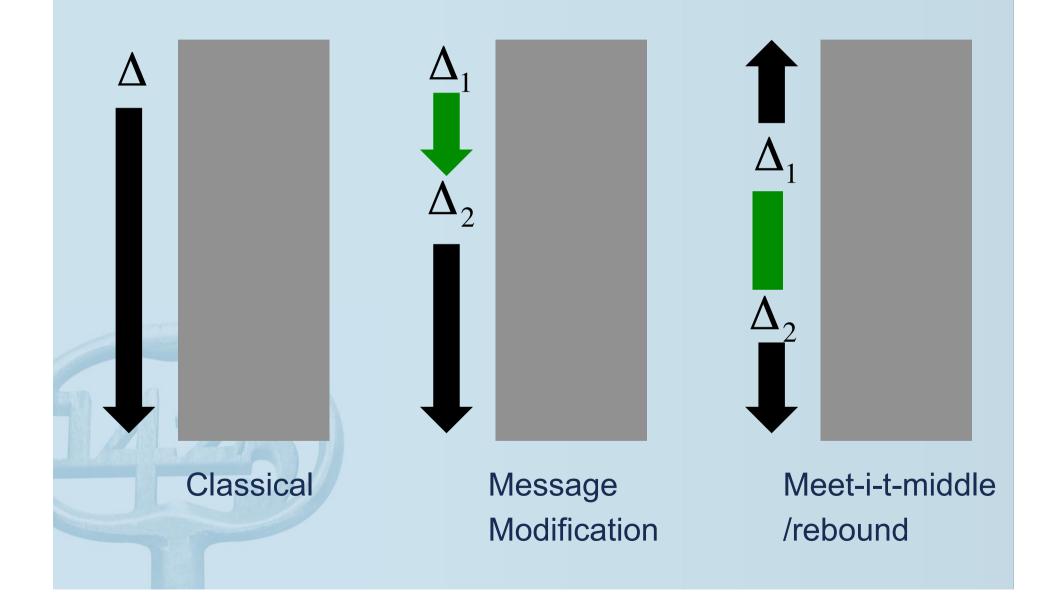
- Differential cryptanalysis on hash functions
 - Look for characteristic ending in difference 0:

$$h(x \oplus \Delta) \oplus h(x) = 0 \Leftrightarrow h(x \oplus \Delta) = h(x)$$

- Every right pair is a collision
- Finding right pairs: since there is no secret key, solving a set of equations deterministically (in principle)

Solving strategies





Attack complexity

- How practical is attack X?
- Number of computations
 - Measured in equivalent hash computations?
- Amount of memory
 - Large memories are slow!
- Complexity of the description
 - Correctness!



Cube distinguishers

• Cube/AIDA/higher order differential: cube tester c

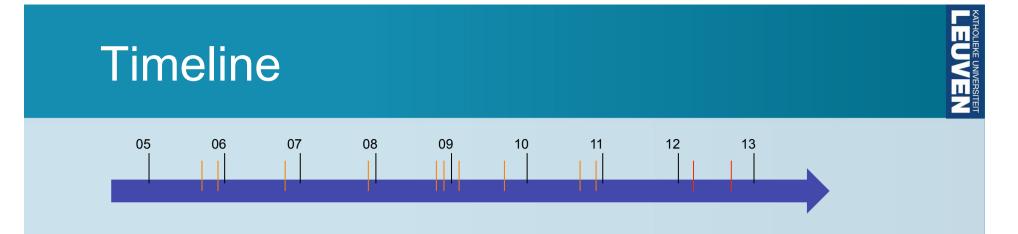
$$c(x) = \sum_{x \in V} f(x)$$

- Look for "special" c:
 - Equal to zero, linear, unbalanced, ...

Cowboy sharpshooter







Mar 2012: 3rd SHA-3 candidate conference Oct 2012: Decision



Outcomes of the SHA-3 competition

- A winner: Keccak
 Or SHA-256?
- Progress in knowledge on hash functions
 And on AES security
- Semi-automatic tools and libraries http://www.ecrypt.eu.org/tools/